

What is claimed is:

1. A computer-based method, comprising:

monitoring the operating system during runtime for an event caused from a request made by a Downloadable; interrupting processing of the request; comparing information pertaining to the Downloadable against a predetermined security policy; and performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing results of the comparison in an event log.

2. A computer-based method, comprising:

monitoring the operating system during runtime for an event caused from a request made by a Downloadable; interrupting processing of the request; comparing information pertaining to the Downloadable against a predetermined security policy; and performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing the Downloadable in a suspicious Downloadable database.

3. A system, comprising:

a security policy; an operating system interface for recognizing a runtime event caused from a request made by a Downloadable; a comparator coupled to the interface for comparing information pertaining to the received Downloadable with the security policy; a response engine coupled to the comparator for performing a predetermined responsive action based on the comparison with the security policy; and an event log coupled to the comparator for storing results of the comparison.

4. A system, comprising:

a security policy; an operating system interface for recognizing a runtime event caused from a request made by a Downloadable; a comparator coupled to the interface for comparing information pertaining to the received Downloadable with the security policy; a response engine coupled to the comparator for performing a predetermined responsive action based on the comparison with the security policy; and a suspicious Downloadable database for storing known and previously-deemed suspicious Downloadables.

5. A system for determining whether a Downloadable, which is received by a Downloadable engine, is suspicious, comprising:

means for monitoring the operating system during runtime for an event caused from a request made by a Downloadable;

means for interrupting processing of the request;

means for comparing information pertaining to the Downloadable against a predetermined security policy; and

means for performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing results of the comparison in an event log.

6. A system for determining whether a Downloadable, which is received by a Downloadable engine, is suspicious, comprising:

means for monitoring the operating system during runtime for an event caused from a request made by a Downloadable;

means for interrupting processing of the request;

means for comparing information pertaining to the Downloadable against a predetermined security policy; and

means for performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing the Downloadable in a suspicious Downloadable database.

7. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

monitoring the operating system during runtime for an event caused from a request made by a Downloadable; interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing results of the comparison in an event log.

8. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

monitoring the operating system during runtime for an event caused from a request made by a Downloadable; interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing the Downloadable in a suspicious Downloadable database.

\* \* \* \* \*